Clandestine Fox, Part Deux

fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html

We reported at the end of April and the beginning of May on an APT threat group leveraging a zero-day vulnerability in Internet Explorer via phishing email attacks. While Microsoft quickly released a patch to help close the door on future compromises, we have now observed the threat actors behind “Operation Clandestine Fox” shifting their point of attack and using a new vector to target their victims: **social networking**.

An employee of a company in the energy sector recently received an email with a RAR archive email attachment from a candidate. The attachment, ostensibly containing a resume and sample software program the applicant had written, was from someone we’ll call “Emily” who had previously contacted the actual employee via a popular social network.

FireEye acquired a copy of the suspicious email – shown below in Figure 1 – and attachment from the targeted employee and investigated. **The targeted employee confirmed that “Emily” had contacted him via the popular social network, and that, after three weeks of back and forth messaging “she” sent her “resume” to his personal email address.**

[caption id="attachment_5658" align="aligncenter" width="441"]

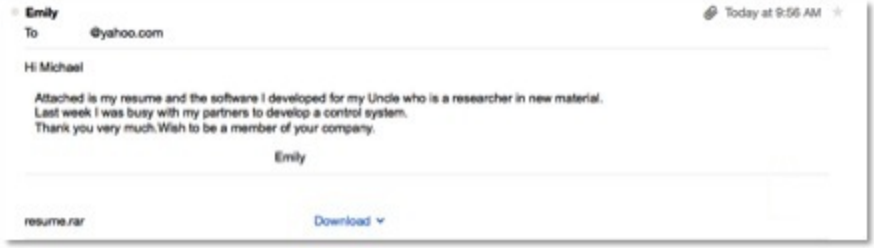

Figure 1: Sample email illustrating how “Emily” attacks a victim employee[/caption]

Working our way backwards, we reviewed “Emily’s” social network profile and noticed a few strange aspects that raised some red flags. For example, “her” list of contacts had a number of people **from the victim’s same employer**, as well as employees from other energy companies; **“she” also did not seem to have many other “friends” that fit “her” alleged persona**. “Her” education history also contained some fake entries.

Further research and discussions with the targeted company revealed that “Emily,” posing as a prospective employee, **had also contacted other personnel at the same company**. She had asked a **variety of probing questions, including inquiring who the IT Manager was and what versions of software they ran** – all information that would be very useful for an attacker looking to craft an attack.

It’s worth emphasizing that in the instances above, the attackers **used a combination of direct contact via social networks as well as contact via email**, to communicate with their intended targets and send malicious attachments. In addition, in almost all cases, **the attackers used the target’s personal email address, rather than his or her work address**. This could be by design, with a view toward circumventing the more comprehensive email security technologies that most companies have deployed, or also due to many people having their social network accounts linked to their personal rather than work email addresses.

Details - Email Attachment #1

The `resume.rar` archive contained three files: a **weaponized** version of the open-source TTCalc application (a mathematical big number calculator), a **benign** text copy of the TTCalc readme file, and a **benign** PDF of Emily’s resume. The resume was a nearly identical copy of a sample resume available elsewhere on the Internet. The file details are below.

Filename	MD5 Hash
resume.rar resume.rar	8b42a80b2df48245e45f99c1bdc2ce51 8b42a80b2df48245e45f99c1bdc2ce51
readme.txt readme.txt	8c6dba68a014f5437c36583bbce0b7a4 8c6dba68a014f5437c36583bbce0b7a4

resume.pdf resume.pdf	ee2328b76c54dc356d864c8e9d05c954 ee2328b76c54dc356d864c8e9d05c954
ttcalc.exe ttcalc.exe	e6459971f63612c43321ffb4849339a2 e6459971f63612c43321ffb4849339a2

Upon execution, `ttcalc.exe` drops the two files listed below, and also launches a legitimate copy of TTCalc v0.8.6 as a decoy:

`%USERPROFILE%/Application Data/mt.dat`

`%USERPROFILE%/Start Menu/Programs/Startup/vc.bat`

The file mt.dat is the actual malware executable, which we detect as **Backdoor.APT.CookieCutter.** (Variants of this family of backdoor are also referred to as "Pirpi" in the security industry). In this case, the malware was configured to use the following remote servers for command and control:

- `swe[.]karasoyemlak[.]com`
- inform[.]bedircati[.]com (**Note: This domain was also used during Operation Clandestine Fox)**
- 122.49.215.108

Metadata for mt.dat:

Description	MD5 Hash
md5 md5	1a4b710621ef2e69b1f7790ae9b7a288 1a4b710621ef2e69b1f7790ae9b7a288
.text .text	917c92e8662faf96fffb8ffe7b7c80fb 917c92e8662faf96fffb8ffe7b7c80fb
.rdata .rdata	975b458cb80395fa32c9dda759cb3f7b 975b458cb80395fa32c9dda759cb3f7b
.data .data	3ed34de8609cd274e49bbd795f21acc4 3ed34de8609cd274e49bbd795f21acc4
.rsrc .rsrc	b1a55ec420dd6d24ff9e762c7b753868 b1a55ec420dd6d24ff9e762c7b753868
.reloc .reloc	afd753a42036000ad476dcd81b56b754 afd753a42036000ad476dcd81b56b754
Import Hash Import Hash	fad20abf8aa4eda0802504d806280dd7 fad20abf8aa4eda0802504d806280dd7

Compile date Compile date	2014-05-27 15:48:13 2014-05-27 15:48:13

Contents of vc.bat:

```
@echo offcmd.exe /C start rundll32.exe "C:\Documents and Settings\admin\Application Data\mt.dat" UpdvaMt
```

Details - Email Attachment #2

Through additional research, we were able to obtain another RAR archive email attachment sent by the same attackers to an employee of another company. Note that while there are a lot of similarities, such as the fake resume and inclusion of TTCalc, **there is one major difference, which is the delivery of a completely different malware backdoor.** The attachment name this time was “my resume and `projects.rar`,” but this time it was protected with the password “`TTcalc`.”

Filename	MD5 Hash
my resume and projects.rar my resume and projects.rar	ab621059de2d1c92c3e7514e4b51751a ab621059de2d1c92c3e7514e4b51751a
SETUP.exe SETUP.exe	510b77a4b075f09202209f989582dbea 510b77a4b075f09202209f989582dbea
my resume.pdf my resume.pdf	d1b1abfcc2d547e1ea1a4bb82294b9a3 d1b1abfcc2d547e1ea1a4bb82294b9a3

`SETUP.exe` is a self-extracting RAR, which opens the WinRAR window when executed, prompting the user for the location to extract the files. It writes them to a TTCalc folder and tries to launch `ttcalcBAK.exe` (the malware dropper), but the path is incorrect so it fails with an error message. All of the other files are benign and related to the legitimate TTCalc application.

Filename	MD5 Hash
CHANGELOG CHANGELOG	4692337bf7584f6bda464b9a76d268c1 4692337bf7584f6bda464b9a76d268c1
COPYRIGHT COPYRIGHT	7cae5757f3ba9fef0a22ca0d56188439 7cae5757f3ba9fef0a22ca0d56188439
README README	1a7ba923c6aa39cc9cb289a17599fce0 1a7ba923c6aa39cc9cb289a17599fce0
ttcalc.chm ttcalc.chm	f86db1905b3f4447eb5728859f9057b5 f86db1905b3f4447eb5728859f9057b5

ttcalc.exe ttcalc.exe	37c6d1d3054e554e13d40ea42458ebed 37c6d1d3054e554e13d40ea42458ebed
ttcalcBAK.exe ttcalcBAK.exe	3e7430a09a44c0d1000f76c3adc6f4fa 3e7430a09a44c0d1000f76c3adc6f4fa

The file `ttcalcBAK.exe` is also a self-extracting Rar which drops and launches `chrome_frame_helper`, **which is a Backdoor.APT.Kaba (aka PlugX/Sogu) backdoor using a legitimate Chrome executable to load the malicious DLL via side-loading**. Although this backdoor is used by multiple threat groups and is quite commonly seen these days, **this is the first time we've observed this particular threat group using this family of malware**. The malware was configured to communicate to the command and control domain `www[.]walterclean[.]com (72.52.83.195` at the time of discovery) using the binary TCP protocol only. The file details are below, followed by the malware configuration.

Filename	MD5 Hash
chrome_frame_helper.dll chrome_frame_helper.dll	98eb249e4ddc4897b8be6fe838051af7 98eb249e4ddc4897b8be6fe838051af7
chrome_frame_helper.dll.hlp chrome_frame_helper.dll.hlp	1b57a7fad852b1d686c72e96f7837b44 1b57a7fad852b1d686c72e96f7837b44
chrome_frame_helper.exe chrome_frame_helper.exe	ffb84b8561e49a8db60e0001f630831f ffb84b8561e49a8db60e0001f630831f

Metadata	MD5 Hash
chrome_frame_helper.dll chrome_frame_helper.dll	98eb249e4ddc4897b8be6fe838051af7 98eb249e4ddc4897b8be6fe838051af7
.text .text	dfb4025352a80c2d81b84b37ef00bcd0 dfb4025352a80c2d81b84b37ef00bcd0
.rdata .rdata	4457e89f4aec692d8507378694e0a3ba 4457e89f4aec692d8507378694e0a3ba
.data .data	48de562acb62b469480b8e29821f33b8 48de562acb62b469480b8e29821f33b8
.reloc .reloc	7a7eed9f2d1807f55a9308e21d81cccd 7a7eed9f2d1807f55a9308e21d81cccd
Import hash Import hash	6817b29e9832d8fd85dcbe4af176efb6 6817b29e9832d8fd85dcbe4af176efb6
Compile date Compile date	2014-03-22 11:08:34 2014-03-22 11:08:34

Backdoor.APT.Kaba Malware Configuration:

PlugX Config (0x150c bytes):

Flags: False True False False False False True True True True False

Timer 1: 60 secs

Timer 2: 60 secs

C&C Address: www[.]walterclean[.]com:443 (TCP)

Install Dir: %ALLUSERSPROFILE%\chrome_frame_helper

Service Name: chrome_frame_helper

Service Disp: chrome_frame_helper

Service Desc: Windows chrome_frame_helper Services

Online Pass: 1234

Memo: 1234

Open Source Intel

The domain `walterclean[.]com` shares registration details with `securitywap[.]com`:

The following domains are registered to QQ360LEE@126.COM

`Domain: walterclean[.]com`

`Create Date: 2014-03-26 00:00:00`

`Registrar: ENOM, INC.`

Domain: securitywap[.]com

Create Date: 2014-03-26 00:00:00

Registrar: ENOM, INC.

Conclusion

In short, we attributed these attacks to the same threat actor responsible for “Operation Clandestine Fox,” based on the following linkages:

- The first-stage malware (mt.dat) is a slightly updated version of the Backdoor.APT.CookieCutter malware dropped during Operation Clandestine Fox

- Based on our intel, Backdoor.APT.CookieCutter has been used exclusively by this particular threat group
- Finally, the command and control domain inform[.]bedircati[.]com seen in this activity was also used during the Clandestine Fox campaign

Another evolutionary step for this threat group is that they have diversified their tool usage with the use of the Kaba/PlugX/Sogu malware – something we have never seen them do before.

As we have noted in other blog posts, APT threat actors take advantage of every possible vector to try to gain a foothold in the organizations they target. Social networks are increasingly used for both personal and business reasons, and are one more potential threat vector that both end-users and network defenders need to think about.

Unfortunately, it is very common for users to let their guard down when using social networks or personal email, since they don't always treat these services with the same level of risk as their work email. As more companies allow their employees to telecommute, or even allow them to access company networks and/or resources using their personal computers, these attacks targeting their personal email addresses pose significant risk to the enterprise.

Acknowledgements

The author would like to acknowledge the following colleagues for their contributions to this report: Josh Dennis, Mike Oppenheim, Ned Moran, and Joshua Homan.